In the Claims

1.   (Withdrawn)   A layered defense-in-depth knowledge-based management system, comprising:

a reception zone for authenticating a user for access to the system;

an operations zone for adjudicating on a user level access to the data objects stored in a system database; and

a security zone for issuing certificates of accessibility for defined users.

2.   (Withdrawn)   A layered defense-in-depth knowledge-based management system as in Claim 1 further comprises revoking certificates for users no longer allowed access to the system.

3.   (Withdrawn)   A layered defense-in-depth knowledge-based management system as in Claim 2, wherein the security zone further comprises performing key recovery operations.

4.   (Withdrawn)   A layered defense-in-depth knowledge-based management system as in Claim 1, wherein the security zone further comprises filters to control and limit access to a predefined set of user workstations.

5.   (Withdrawn)   A layered defense-in-depth knowledge-based management system as in Claim 1, wherein the reception zone comprises a public key infrastructure for authenticating users for accessing contents of the system.

6.   (Withdrawn)   A layered defense-in-depth knowledge-based management system, comprising:

a reception zone for authenticating a user for access to the system;

a screening zone to interrogate data packets during processing thereof;

an operations zone for adjudicating on the user level access to the data objects stored in a system database; and

a security zone for issuing certificates of accessibility for defined users, revoke certificates for users no longer allowed access to the system, and performing key recovering operations.

7.   (Withdrawn)   A layered defense-in-depth knowledge-based management system as set forth in Claim 6, wherein the reception zone comprises a public key infrastructure for authenticating users for accessing contents of the system.

8.   (Withdrawn)   A layered defense-in-depth knowledge-based management system as in Claim 6, wherein the operations zone comprises packet filtering for incoming and outgoing messages.

9.   (Withdrawn)   A layered defense-in-depth knowledge-based management system as in Claim 6, wherein the security zone comprises packet filtering of incoming and outgoing messages for access control.

10.   (Withdrawn)   A layered defense-in-depth knowledge-based management system as in Claim 6, wherein the operations zone comprises a document management server for establishing access to data stored in a library of the management system.

11. (Currently Amended) A method of layered defense-in-depth knowledge-based management, comprising:

authenticating a user of the knowledge base;

determine the clearance level of a requested document ~~by the authenticated user~~ and at least one document caveat of the requested document, the at least one document caveat representing a necessary condition for access to the document;

determine the clearance level of the authenticated user and at least one user caveat of the authenticated user, the at least one user caveat representing a condition necessary for the authenticated user to have access to a document having an associated at least one document caveat;

comparing the clearance level of the document with the clearance level of the authenticated user; ~~and~~

comparing the at least one document caveat of the requested document to the at least one user caveat of the authenticated user; and

displaying the secure document to the authenticated user in response to the clearance level of the user dominating the clearance level of the requested document and the comparison of the at least one document caveat of the requested document to the at least one user caveat of the authenticated user.

12. (Cancelled)

13. (Original) The method of layered defense-in-depth knowledge-based management as in Claim 11, further comprising encrypting and signing the authenticated user prior to determining the clearance level of a requested document.

14. (Original) The method of layered defense-in-depth knowledge-based management as in Claim 11, wherein authenticating a user comprises a certificate authority program running on a server.

15. (Currently Amended) A method of layered defense-in-depth knowledge-based management, comprising:

authenticating a user of the knowledge base;

determine the clearance level of a requested secure document;

determine the clearance level of the authenticated user;

comparing the clearance level of the requested document with the clearance level of the authenticated user;

obtaining a document caveat, the document caveat representing a necessary condition for access to the document;

obtaining an authenticated user caveat, the user caveat representing a condition necessary for a user associated with the user caveat to have access to a document having an associated document caveat;

comparing the authenticated user caveat with the document caveat to allow access to the obtained document caveat;

determining the access allowability of the obtained document caveat;

determining the allowance of both the document caveat and the clearance access to identify clearance of the authorized user to the requested secure document; and

displaying the secure document to the authenticated user.

16. (Original) The method of layered defense-in-depth knowledge-based management as in Claim 15, further comprising multiple authentication of a user prior to comparing the clearance level of the requested document with the clearance level of the authenticated user.

17. (Withdrawn) A method of accessing an electronic support library for layered defense-in-depth knowledge-based management, comprising:

authenticating in a reception zone a user in response to a request for data;

document manipulation and administration in an operations zone of a request by an authenticated user; and

issuing authorization certificates in a security zone for users to allow access to data managed in the operations zone.

18. (Withdrawn) The method of accessing an electronic support library as in Claim 17, wherein authenticating a user in the reception zone comprises authenticating the user to a public key infrastructure.

19. (Withdrawn) The method of accessing an electronic support library as in Claim 17, further comprising accessing data stored in the electronic support library by a document management server.

20. (Withdrawn) The method of accessing an electronic support library as in Claim 17, further comprising packet filtering incoming and outgoing messages in and through the operations zone.

21. (Withdrawn) The method of accessing an electronic support library as in Claim 20, further comprising packet filtering incoming and outgoing messages for access to authorization certificates issued by the security zone.